



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

78

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,081	10/30/2001	David M. Blaker	5601-003	9375

7590 06/27/2006

David E. Bennett  
Coats & Bennett, P.L.L.C.  
P.O. Box 5  
Raleigh, NC 27602

EXAMINER

PICH, PONNOREAY

ART UNIT PAPER NUMBER

2135

DATE MAILED: 06/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/004,081

Applicant(s)

BLAKER, DAVID M.

Examiner

Ponnoreay Pich

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 14 April 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-9 and 16-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-9 and 16-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/14/2006 has been entered.

Claims 1-9 and 16-33 are pending.

### ***Response to Amendment and Arguments***

Applicant's amendments and remarks/arguments have been fully noted. Any objections or rejections not repeated below for record and not specifically addressed are withdrawn due to applicant's amendments and/or arguments.

Applicant argues that the 101 rejections of claims 1 and 25 should be withdrawn because the claims have been amended to indicate that the stream cipher comprises a logical combination of the random values and plaintext and that the claims as a whole accomplishes a practical application which produces a concrete, useful, and tangible result. The examiner respectfully disagrees. The examiner notes that applicant also made comments that the claims are not devoid of any limitations to a practical application in the technology arts. The examiner assumes applicant may not be aware that the Office issued an Interim Guideline for 101 Analysis (herein Interim Guidelines) in October 2005 since applicant seems to be applying the test of whether an invention is within the technological arts to determine patentability. This test was discussed as

Art Unit: 2135

being an improper test for determining patentability in the Interim Guidelines (see Annex III(a) of Interim Guidelines). The examiner respectfully submits that even with the amendments, the claims previously rejected under 101 are not statutory. Claim 1 directed towards a method of determining random values for a stream cipher.

Applicant's amendment that the stream cipher comprises a logical combination of the random values and plaintext still does not indicate that the random values were used to create a stream cipher. Instead, it appears that the method is intended to be used for a stream cipher and if it was used for a stream cipher, the stream cipher would comprise a logical combination of the random values and plaintext. There is no step which actually states that the random values were definitely used to generate the stream cipher. The examiner notes that if applicant adds such a step to the claim, claim 1 would be statutory because the method then has a result that is concrete, useful, and tangible. As per claim 25, the claim is directed towards a computer program product which is a computer readable media comprising program code. Applicant's specification clearly defines a computer readable media as being a signal, thus the claim is not statutory since a signal is not classifiable in any of the statutory categories as defined by 35 USC 101, see Annex IV(c) of Interim Guidelines for further discussion. Note that any 101 rejections made in this office action are made in light of what is disclosed in the Interim guidelines, which are based on the Office's current understanding of the law and are believed to be fully consistent with binding precedent of the Supreme Court, the Federal Circuit, and the Federal Circuit's predecessor courts.

The rest of applicant's arguments are moot in view of new rejections presented below.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-9 and 16-33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claims 1, 16, and 35 have been amended to recite "the stream cipher comprising a logical combination of the random values and plaintext". However, it is unclear if the clause further limits the claims since "for a stream cipher" in the preamble indicates an intended use and the clause appears to be directed towards an intended stream cipher rather than one that actually exists. Thus, it appears that the intended stream cipher comprises a logical combination of the random values and plaintext. The examiner believes that if applicant has a limitation in claims 1, 16, and 25 which actually states using the random values to create the stream cipher, then the stream cipher would be considered an actual stream cipher.
2. Claim 25 recites computer readable program code comprising: "a memory..." and "computer readable program code...". It is unclear how code can comprise memory and how code can comprise code.
3. Any claims not specifically addressed are rejected by virtue of dependency.

***Claim Rejections - 35 USC § 101***

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-9 and 25-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

1. Claim 1 is directed towards a method of determining a random value for a stream cipher. Note that determining a random value is a computation in a computer and that no concrete, useful, and tangible result has been produced by the step recited in claim 1. Applicant can make claim 1 statutory by reciting in an appropriate manner that the random values were used to produce the stream cipher.
2. Claims 2-9 are dependent on claim 1 and also do not appear to produce a concrete, useful, and tangible result.
3. Claim 25 refers to a computer program product comprising a computer readable media. The examiner notes that on page 6, lines 31-33, applicant defines a computer-readable medium as including "an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium." As such, the computer-readable media recited in claim 25 reads on a signal. It is the Office's current view that signals do not constitute patent-eligible subject matter. Claim 25 also does not recite any tangible result. The examiner notes that if applicant did not define a computer readable storage

Art Unit: 2135

media as a signal in the specification, the computer program product of claim 25 comprising a computer readable storage media and execution of the code providing a useful, concrete, and tangible result would be statutory.

4. Claims 26-33 are dependent on claim 25 and also are directed towards a computer program product being a signal, thus are not statutory.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 16, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan et al (US 6,490,354) in view of Chiu et al (US 4,667,301).

#### **Claims 1, 16, and 25:**

As per claim 1, Venkatesan discloses determining at least two sequential random values utilizing a common S-box (Fig 6; col 9, lines 31-57; and col 11, lines 22-25). Venkatesan discloses the stream cipher comprising a logical combination of the random values and plaintext (col 2, lines 8-11 and col 3, lines 38-42). Note that even had Venkatesan not disclosed the stream cipher comprising a logical combination of the random values and plaintext, one skilled in the art of cryptography should appreciate

Art Unit: 2135

that ciphertexts, i.e. stream ciphers, are created by combining the key material, i.e. random value, with a plaintext.

Venkatesan does not disclose the determining was done in parallel. However, determination of random values in parallel is disclosed by Chiu (col 2, lines 1-4). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Venkatesan's invention according to the limitations recited in claim 1 such that the determining was done in parallel utilizing a common S-box in light of Chiu's teachings. One skilled would have been motivated to do so because parallel computation would allow higher throughput and allow random numbers to be generated much faster for use as key material. Note that this would allow encryption to also be faster.

Claims 16 and 25 recite limitations substantially similar to claim 1. The difference is that claim 16 refers to a system which implements the method of claim 1 and claim 25 refers to a computer program product with means and computer readable media having computer readable program code therein, to implement the method of claim 1.

Another difference is that claims 16 and 25 explicitly recite a memory containing an S-box. This limitation is also implicitly disclosed by Venkatesan (col 10, line 8-col 11, line 5). Claims 16 and 25 are rejected for substantially the same reasons given for claim 1.



Claims 2-3, 6-7, 17-18, 21-22, 26-27, and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan et al (US 6,490,354) in view of Chiu et al (US 4,667,301) and further in view of Klug et al (US 5,528,526).

**Claims 2, 17, and 26:**

Claims 17 and 26 are substantially similar to claim 2. Claim 17 differs from claim 2 in that claim 17 recites a system with means for implementing the method of claim 2. Claim 26 differ in that it recites a computer program product with computer readable program code for implementing the method of claim 2.

As per claims 2, 17, and 26, Venkatesan further discloses accesses of the common S-box utilized to determine a first of the two sequential random values and access of the common S-box utilized to determine a second of the two sequential random values (Fig 6; col 9, lines 31-57; and col 11, lines 22-25). Venkatesan's invention is used with a stream cipher, so the numbers in the stream of numbers generated by Venkatesan's random number generator are all random numbers.

Venkatesan does not disclose:

1. Determining if a collision exists between accesses.
2. Modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box.

However, Klug discloses determining if a collision/cycle exists between in the generation of random numbers (col 3, lines 21-35). Note that each symbol disclosed by Klug in the pattern supplied on bus 18 reads on a random number. In light of this, it

Art Unit: 2135

would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Venkatesan's invention to determine if a collision exists between accesses of the common S-box utilized to determine a first of the two sequential random values and access of the common S-box utilized to determine a second of the two sequential random values. One of ordinary skill would have been motivated to do so as Klug discloses that by detecting short cycle patterns (collisions), many diverse failure modes associated with random number generators may be identified.

Klug also does not explicitly disclose modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box. However, this limitation is obvious to the combination of Venkatesan and Klug as the reason Klug wanted to detect collision or repeating patterns in random number generation was to determine if an error is present in the generation process. If an error is present, it is obvious to one of ordinary skill to modify the determination of the random values as recited in claims 2, 17, and 26. One of ordinary skill would have been motivated to modify the determination, as it would correct the errors disclosed by Klug.

**Claims 6, 21, and 30:**

Claims 21 and 30 are substantially similar to claim 6. Claim 21 differs from claim 6 in that claim 21 recites a system with means for implementing the method of claim 6. Claim 30 differ in that it recites a computer program product with computer readable program code for implementing the method of claim 6.

As per claims 6, 21, and 30, Venkatesan does not disclose:

1. Determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the first of the two sequential random values.
2. Determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the two sequential random values.

However, the above limitations are obvious to the combination of Venkatesan, Chiu, and Klug. Venkatesan's invention deals with generating a stream of random numbers (in byte format) for encryption purposes (col 1, lines 9-12). Klug deals with detecting collisions or pattern repeats within a sequence of numbers/symbols (col 1, lines 8-12). It is obvious that the combination invention of Venkatesan, Chiu, and Klug would be able to detect collisions within any random value comprising a first and second portion as the combination invention looks for collisions within the streams itself rather than just one number with another number. The examiner also notes that within the stream generated, it is arbitrary where one "number" begins and ends as it depends on the system the random number generator is used how many bits or bytes comprise a number.

**Claims 3, 7, 18, 22, 27, and 31:**

Venkatesan does not explicitly disclose:

1. Determining a state associated with the determination of the at least two sequential random values.
2. Comparing values of counters utilized in determining the at least two sequential random values.
3. Detecting a collision based on the determined state and the compared values.

However, the above limitations are obvious to the combination invention of Venkatesan, Chiu, and Klug. Klug discloses that once a collision is first detected, more tests are needed to determine if the collision is a false repeat or not (Fig 2; Fig 5; and col 6, line 45-col 7, line 40). Each level of testing for a match reads on a separate state as disclosed by Klug. To determine absolutely that the pattern detected is not a false collision, the state must be determined to be the final level of verification (Fig 5, items 82 and 84).

#### ***Allowable Subject Matter***

Claims 4-5, 8-9, 19-20, 23-24, 28-29, and 32-33 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 101 and 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims. The claims are allowable for the same reasons as given in the prior office action.

***Conclusion***


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich  
Examiner  
Art Unit 2135

PP

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER